Amendments to the Specification:

Please replace the paragraph beginning on page 7, line 18, with the following amended paragraph:

In accordance with the present invention, the cipher key (Ks) used to encipher the data (M) requested by a communication terminal can only be obtained by decoding the personal secret key ({Ks}Kh) generated in accordance with an enciphering operation of the (Ks) enciphering unit, by using the hidden secret key (Kh) intrinsically assigned to the communication terminal. Accordingly, although enciphered data is circulated over public networks, its original data can be secured. Thus, an improvement in data security is achieved.

Please replace the paragraph beginning on page 9, line 7, with the following amended paragraph:

Fig. 1 is a block diagram illustrating a data service providing apparatus according to a preferred embodiment of the present invention. As shown in Fig. 1, the data service providing apparatus, which is denoted by the reference numeral 100, includes a control unit 110, a database 120 for storing data (M) (hereinafter, referred to as an "(M) database"), a database 130 for storing hidden secret keys (Kh) (hereinafter, referred to as a "(Kh) database"), a transmitting/receiving unit 140, an enciphering unit 150 for data (M) (hereinafter, referred to as an "(M) enciphering unit"), and an enciphering unit 160 for a cipher key (Ks) (hereinafter, referred to as a "(Ks) enciphering unit"). ~~[PLEASE CORRECT FIG. 1 AS SHOWN]~~ The data service providing apparatus 100 communicates with a communication terminal 200 via a public network 50.

On page 9, please replace the paragraph beginning on line 17 with the following paragraph:

The control unit 110 controls the operation of the data service providing apparatus 100. The (M) database 120 stores data (M) to be supplied to the communication terminal 200, and transfers the stored data M to the control unit 110 under the control of the control unit 110.

Generally, the data {M} includes commercial data and secured data. The {Kh} database 130 stores hidden secret keys {Kh} each corresponding to intrinsic identification (ID) information of a security deciphering module 400 equipped in the communication terminal 200, and adapted to decipher enciphered data. The {Kh} database 130 transfers a selected one of the stored hidden secret keys {Kh} to the control unit 110 under the control of the control unit 110.

Please replace the paragraph beginning on page 10, line 2, with the following amended paragraph:

The transmitting/receiving unit 140 communicates with the communication terminal 200 via the public network 50 under the control of the control unit 110. The {M} enciphering unit 150 enciphers the data {M} stored in the data database 120, using a cipher key {Ks}, under the control of the control unit 110. The {Ks} enciphering unit 160 enciphers the cipher key {Ks} used to encipher the data {M}, using the hidden secret key {Kh} stored in the {Kh} database 130, under the control of the control unit 110.

Please replace the paragraph beginning on page 10, line 8, with the following amended paragraph:

The transmitting/receiving unit 140 transmits enciphered data outputted from the {M} enciphering unit 150, that is, enciphered data {{M}Ks}, and an enciphered cipher key ~~outputted~~ output from the {Ks} enciphering unit 160, that is, a personal secret key {{Ks}Kh} ({Ks}Kh = Kp), to the communication terminal 200 requesting the data {M} via the public network 50.

Please replace the paragraph beginning on page 10, line 13, with the following amended paragraph:

As the enciphered data {{M}Ks} and personal secret key {{Ks}Kh} generated in accordance with respective enciphering operations of the {M} enciphering unit 150 and {Ks} enciphering unit 160 are transmitted to the communication terminal 200 via the public

network 50, it is possible for the data to be made commercially available while maintaining its security.

Please replace the paragraph beginning on page 10, line 21, with the following amended paragraph:

In accordance with the data service providing method, the control unit 110 first determines whether or not there is a data request signal requesting transmission of the data {M} received from a communication terminal, for example, the communication terminal 200, via the transmitting/receiving unit 140 (Step S100). When it is determined that no data request signal is received, the control unit 110 is maintained in a state of waiting for providing of data services (Step S180).

Please replace the paragraph beginning on page 11, line 6, with the following amended paragraph:

When it is determined that the data request signal is received, the control unit 110 reads out the data {M} meeting the data request from the {M} database 120, and then controls the {M} enciphering unit 150 in order to encipher the read-out data {M} by a predetermined cipher key {Ks} (Step S120). The control unit 110 reads out, from the {Kh} database 130, a hidden secret key {Kh} corresponding to the intrinsic ID information of the security deciphering module 400 included in the communication terminal 200, and then controls the {Ks} enciphering unit 160 in order to encipher the cipher key {Ks} used to encipher the data {M} (Step S140).

Please replace the paragraph beginning on page 11, line 14, with the following amended paragraph:

The control unit 110 controls the transmitting/receiving unit 140 in order to transmit the enciphered data {{M}Ks} and personal secret key {{Ks}Kh} to the communication terminal 200 via the public network 50 (Step S160). In accordance with the control operation of the control

unit 110, the transmitting/receiving unit 140 transmits the enciphered data [{M}Ks] and personal secret key [{Ks}Kh] to the communication terminal 200 via the public network 50.

Please replace the paragraph beginning on page 11, line 20, with the following amended paragraph:

Thus, it is possible for the data to be made commercially available while maintaining its security because the enciphered data [{M}Ks] and personal secret key [{Ks}Kh] generated in accordance with respective enciphering operations of the (M) enciphering unit 150 and (Ks) enciphering unit 160 are transmitted to the communication terminal 200 via the public network 50.

Please replace the paragraph beginning on page 12, line 2, with the following amended paragraph:

Fig. 3 is a block diagram illustrating a detailed configuration of the communication terminal 200 shown in Fig. 1. ~~[PLEASE CORRECT FIG. 3 AS SHOWN.]~~ As shown in Fig. 3, the communication terminal 200 includes a control unit 210, a key input unit 230, a display unit 250, a memory 270, a transmitting unit 290, a receiving unit 330, a duplexer 310, a voice processing unit 350, and a voice storing unit 370, in addition to the security deciphering module 400. Also shown are speaker SPK, microphone MIC, and antenna ANT.

Please replace the paragraph beginning on page 12, line 16, with the following amended paragraph:

The memory 270 stores a control program for the communication terminal 200 and the control data generated in accordance with the control operation of the control unit 210. The security deciphering module 400 deciphers the enciphered data [{M}Ks] and personal secret key [{Ks}Kh] transmitted from the data service providing apparatus 100, thereby recovering data (M). The transmitting unit 290 receives a signal generated from the control unit 210, modulates the received signal into a digital radio signal, and transfers the radio signal to the duplexer 310.

The duplexer 310 sends out the radio signal received from the transmitting unit 290 via the antenna, and transfers a signal received via the antenna to the receiving unit 330. The receiving unit 330 demodulates the radio signal received from the duplexer 310, and transfers the demodulated signal to the control unit 210 which, in turn, controls an operation of the communication terminal 200 associated with call services, in response to the demodulated signal.

Please replace the paragraph beginning on page 13, line 14, with the following amended paragraph:

The control unit 210 receives enciphered data {{M}Ks} and a personal secret key {{Ks}Kh} transmitted from the data service providing apparatus 100 in response to the data transmission request signal, and deciphers them, thereby recovering data {M}.

Please replace the paragraph beginning on page 14, line 1, with the following amended paragraph:

The {Kp} storing unit 410 stores a personal secret key {{Ks}Kh} transmitted from the transmitting/receiving unit 140 of the data service providing apparatus 100 shown in Fig. 1 and received by the receiving unit 330 of the communication terminal 200. Under the control of the first decoding unit 450, the personal secret key {{Ks}Kh} stored in the {Kp} storing unit 410 is subsequently outputted to the first decoding unit 450. The {Kh} storing unit 430 stores a hidden secret key {Kh} corresponding to the intrinsic ID information assigned to the security deciphering module 400. Using the hidden secret key {Kh} stored in the {Kh} storing unit 430, the first decoding unit 450 decodes the personal secret key {{Ks}Kh} received from the {Kp} storing unit 410, as expressed by the following Expression {1}, thereby generating decoded data, that is, a cipher key {Ks}. As described above, the personal secret key {{Ks}Kh} is enciphered data generated in accordance with an enciphering operation of the {Ks} enciphering unit 160 of the data service providing apparatus 100 carried out for the cipher key {Ks}.

Please replace the paragraph beginning on page 14, line 14, with the following amended paragraph:

Expression (1)

$$\{\{\{Ks\}Kh\}Kh\} = \{Ks\}$$

Please replace the paragraph beginning on page 14, line 16, with the following amended paragraph:

The {Ks} storing unit 470 stores the decoded data outputted from the first decoding unit 450, that is, the cipher key {Ks}. Under the control of the second decoding unit 490, the cipher key {Ks} stored in the {Ks} storing unit 470 is subsequently transferred to the second decoding unit 490. Using the cipher key {Ks} outputted from the {Ks} storing unit 470, the second decoding unit enciphered data {{M}Ks} generated from the {M} enciphering unit 150 of the data service 490 decodes providing apparatus 100, as expressed by the following Expression (2).

Please replace the paragraph beginning on page 15, line 1, with the following amended paragraph:

Expression (2)

$$\{\{\{M\}Ks\}Ks\} = \{M\}$$

Please replace the paragraph beginning on page 15, line 6, with the following amended paragraph:

Fig. 5 is a flow chart illustrating a method for deciphering enciphered data by using the above described security deciphering apparatus in accordance with a preferred embodiment of the present invention. In accordance with this method, the control unit 210 of the communication terminal 200 first determines whether or not there is a personal secret key

[{Ks}Kh] ([{Ks}Kh] = [Kp]) received from the data service providing apparatus 100 (Step S200). When it is determined that the personal secret key [{Ks}Kh] is received, the control unit 210 stores the personal secret key [{Ks}Kh] in the [Kp] storing unit 410 (Step 220).

Please replace the paragraph beginning on page 15, line 14, with the following amended paragraph:

The first decoding unit 450 then decodes the personal secret key [{Ks}Kh] stored in the [Kp] storing unit 410, using the hidden secret key [Kh] stored in the [Kh] storing unit 430, thereby generating decoded data, that is, a cipher key [Ks] (Step S240). The cipher key [Ks] generated from the first decoding unit 450 is stored in the [Ks] storing unit 470 (Step S260).

Please replace the paragraph beginning on page 15, line 19, with the following amended paragraph:

The control unit 210 subsequently determines whether or not there is enciphered data [{M}Ks] received from the data service providing apparatus 100 (Step 280). When it is determined that the enciphered data [{M}Ks] is received, the second decoding unit 490 decodes the enciphered data [{M}Ks], using the cipher key [Ks] stored in the [Ks] storing unit 470, thereby generating decoded data, that is, data [M] (Step S320).

Please replace the paragraph beginning on page 16, line 5, with the following amended paragraph:

Thus, it is possible to receive the data M in a secured state as the data [M] is recovered in accordance with the decoding operations for the enciphered data [{M}Ks] and personal secret key [{Ks}Kh] carried out by the first and second decoding units 450 and 490.

Please replace the paragraph beginning on page 16, line 9, with the following amended paragraph:

As apparent from the above description, the cipher key (Ks) used to encipher the data (M) requested by a communication terminal can only be obtained by decoding the personal secret key ({Ks}Kh) generated in accordance with an enciphering operation of the (Ks) enciphering unit, by using the hidden secret key (Kh) intrinsically assigned to the communication terminal. Accordingly, although enciphered data is circulated over public networks, its original data can be secured. Thus, an improvement in data security is achieved.